CLAIMS

1. A certification method using a public key certification authority (30) and involving at least one mobile terminal (10) able to receive messages encrypted by that public key, characterized in that it includes the step of the mobile terminal (10) generating the public key, the step of a telecommunications network entity (20) acquiring said key from the terminal (10) by means of a network call, the step of the network entity authenticating the terminal (10) by a party authentication process used in relation to a standard telephone call, and the step of supplying the certification authority (30) with the public key and the associated result of the authentication process.

2. A method according to claim 1, characterized in that the step of authenticating the mobile (10) includes the mobile (10) sending a calculation result involving a confidential key stored in the mobile and the step of the network entity (20) comparing the result with an expected result also calculated by the network entity (20) using the same confidential key, a positive comparison result being interpreted as an identification of the mobile terminal.

3. A method according to claim 2, characterized in that it comprises the step of the network entity sending random data to the terminal and the step of the terminal calculating the random data sent by the network entity, the step of calculation by the network entity also involving said random data with a view to said comparison of results.

4. A method according to any preceding claim, characterized in that it includes the step of the mobile terminal (10) generating, in addition to the public key, a confidential key held in memory in the mobile (10) and

used to decrypt received messages that were encrypted with the public key.

5. A method according to claim 4, characterized in that the terminal is adapted to send messages and to append to them an authentication signature produced using the confidential key that it previously generated itself.

6. A method according to any preceding claim, characterized in that it comprises the step of the network entity (20) sending the public key to the certification authority (30) via a channel that is secured against unauthorized reading.

7. A method according to any preceding claim, characterized in that it comprises the step of the mobile (10) using an authentication key of the mobile (10) usually employed in relation to telephone calls, generating an encryption key, encrypting messages using that encryption key and sending said messages.

8. A mobile telecommunications system comprising at least one mobile terminal (10) and one network entity (20), characterized in that it includes means in the mobile terminal (10) for generating a public key, means in the telecommunications network entity (20) for acquiring said public key from the terminal (10) by means of a network call, and means for authenticating the terminal by means of an authentication process used in relation to a standard telephone call, the system further including a certification authority and means for supplying the certification authority with the public key generated by the mobile terminal and the associated result of the authentication process.

9. A mobile telecommunications terminal (10), characterized in that it includes means for producing at

least one key for decrypting messages received by the terminal and means for sending said key to a certification authority (30) by means of a network call via a telephone network entity (20) so that said key becomes a public key.